配置PIX 5.1.x:TACACS+和RADIUS

目錄

簡介

可以對FTP、Telnet和HTTP連線執行RADIUS和TACACS+身份驗證。對其他不太常用的協定的身份驗證通常可以正常工作。支援TACACS+授權；RADIUS授權不是。PIX 5.1身份驗證、授權和記帳(AAA)與先前版本相比的變化包括擴展身份驗證(xauth) — 從Cisco安全VPN客戶端1.1對IPSec隧道的身份驗證。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

驗證與授權

- 身份驗證是使用者。
- 授權是使用者可以執行的操作。
- 未經授權,身份驗證有效。
- 未經*驗證的*授權無效。
- 記帳是使用者執行的操作。

假設您內部有100個使用者，並且只希望其中六個使用者能夠在網路外部執行FTP、Telnet或HTTP。您會通知PIX驗證出站流量，並為TACACS+/RADIUS安全伺服器上的所有六個使用者ID提供證書。使用簡單身份驗證時，這六個使用者可以使用使用者名稱和密碼進行身份驗證，然後退出。其他94個使用者無法出門。PIX提示使用者輸入使用者名稱/密碼，然後將其使用者名稱和密碼傳遞到TACACS+/RADIUS安全伺服器，並根據響應開啟或拒絕連線。這六個使用者可以執行FTP、Telnet或HTTP。

但假設*這*六個使用者中的一個「Festus」不可信。您想允許Festus執行FTP，而不是通過HTTP或Telnet到外部。這意味著必須新增*授權*，即，除了驗證使用者身份外，還要對使用者能夠執行的操作進行授權。這隻對TACACS+有效。向PIX新增*授權*時，PIX首先將Festus的使用者名稱和密碼傳送到安全伺服器，然後向安全伺服器傳送授權請求，通知Festus嘗試執行的「*command*」操作。正確設定伺服器後，可以允許Festus「ftp 1.2.3.4」，但會拒絕在任何地方使用HTTP或Telnet。

使用者透過開啟驗證/授權看到的專案

當嘗試從內部到外部（反之亦然）並且身份驗證/授權開啟時：

- **Telnet** — 使用者看到使用者名稱提示出現，然後請求密碼。如果在PIX/伺服器上成功進行身份驗證（和授權），則目標主機將提示使用者輸入使用者名稱和密碼。
- **FTP** — 使用者看到使用者名稱提示啟動。使用者需要輸入**local_username@remote_username**作為使用者名稱，輸入**local_password@remote_password**作為密碼。PIX將local_username和local_password傳送到本地安全伺服器，如果在PIX/伺服器上成功進行身份驗證（和授權），則remote_username和remote_password將傳遞到目標FTP伺服器。
- **HTTP** -瀏覽器中將顯示一個要求輸入使用者名稱和密碼的視窗。如果身份驗證（和授權）成功，則使用者將超出該時間到達目標網站。請記住，瀏覽器*會快取使用者名稱和密碼*。如果PIX似乎應該對HTTP連線進行超時，但並未這樣做，則可能實際上在瀏覽器向PIX傳送快取的使用者名稱和密碼時進行了重新身份驗證，然後PIX再將其轉發到身份驗證伺服器。PIX系統日誌和/或伺服器調試顯示了此現象。如果Telnet和FTP似乎工作正常，但HTTP連線不正常，這就是原因。
- **Tunnel** — 當嘗試通過VPN客戶端和xauth將IPSec流量通道化到網路時，對於使用者名稱/密碼，顯示「User Authentication for New Connection」的灰色框。**注意：**從Cisco Secure VPN Client 1.1開始支援此身份驗證。如果**Help > About選單未顯示2.1.x版或更高版本，則此操作不起作用。**

適用於所有場景的安全伺服器配置

Cisco Secure UNIX TACACS伺服器配置

本節提供用於配置安全伺服器的資訊。

確保您在CSU.cfg檔案中具有PIX IP地址或完全限定域名和金鑰。

```
user = ddunlap {
password = clear "rtp"
default service = permit
}

user = can_only_do_telnet {
password = clear "telnetonly"
service = shell {
cmd = telnet {
permit .*
}
}
}

user = can_only_do_ftp {
password = clear "ftponly"
service = shell {
cmd = ftp {
permit .*
}
}
}
```

```
user = httponly {
password = clear "httponly"
service = shell {
cmd = http {
permit .*
}
}
}
```

Cisco Secure UNIX RADIUS伺服器配置

使用GUI將PIX IP地址和金鑰新增到網路訪問伺服器(NAS)清單中。

```
user=adminuser {
radius=Cisco {
check_items= {
2="all"
}
reply_attributes= {
6=6
}
}
}
```

適用於Windows 2.x RADIUS的Cisco安全ACS

使用以下步驟配置適用於Windows 2.x RADIUS的Cisco Secure ACS。

1. 在使用者設定GUI部分獲取密碼。
2. 在Group Setup GUI部分，將屬性6(Service-Type)設定為**Login**或**Administrative**。
3. 在NAS配置部分GUI中新增PIX IP地址。

EasyACS TACACS+

EasyACS文檔描述了設定。

1. 在組部分中，按一下**Shell exec**以授予exec許可權。
2. 要向PIX新增授權，請按一下組設定底部的**Deny unmatched IOS commands**。
3. 為您希望允許的每個命令選擇**Add/Edit new command**，例如**Telnet**。
4. 如果允許Telnet到特定站點，請以「permit #.#.#.#」的形式填寫引數部分的IP地址。 否則，要允許Telnet，請按一下**Allow all unlisted arguments**。
5. 按一下**完成編輯命令**。
6. 對每個允許的命令（例如Telnet、HTTP或FTP）執行步驟1至5。
7. 在NAS配置GUI部分新增PIX IP。

Cisco Secure 2.x TACACS+

使用者在「使用者設定GUI」部分獲得密碼。

1. 在組部分中，按一下**Shell exec**以授予exec許可權。
2. 要向PIX新增授權，請在組設定底部按一下**Deny unmatched IOS commands**。
3. 為您希望允許的每個命令(例如**Telnet**)選擇**Add/Edit new**命令。

4. 要允許Telnet到特定站點，請在引數部分以「permit #.#.#.#」的形式輸入IP地址。 要允許Telnet到任何站點，請按一下**Allow all unlisted arguments**。
5. 按一下**完成編輯命令**。
6. 對每個允許的命令（例如Telnet、HTTP或FTP）執行步驟1至5。
7. 確保在NAS配置GUI部分新增PIX IP地址。

Livingston RADIUS伺服器配置

將PIX IP地址和金鑰新增到Clients檔案。

```
adminuser Password="all" User-Service-Type = Shell-User
```

價值RADIUS伺服器配置

將PIX IP地址和金鑰新增到Clients檔案。

```
adminuser Password="all" Service-Type = Shell-User
```

TACACS+免費軟體伺服器配置

```
key = "cisco"
user = adminuser {
login = cleartext "all"
default service = permit
}

user = can_only_do_telnet {
login = cleartext "telnetonly"
cmd = telnet {
permit .*
}
}

user = httponly {
login = cleartext "httponly"
cmd = http {
permit .*
}
}

user = can_only_do_ftp {
login = cleartext "ftponly"
cmd = ftp {
permit .*
}
}
```

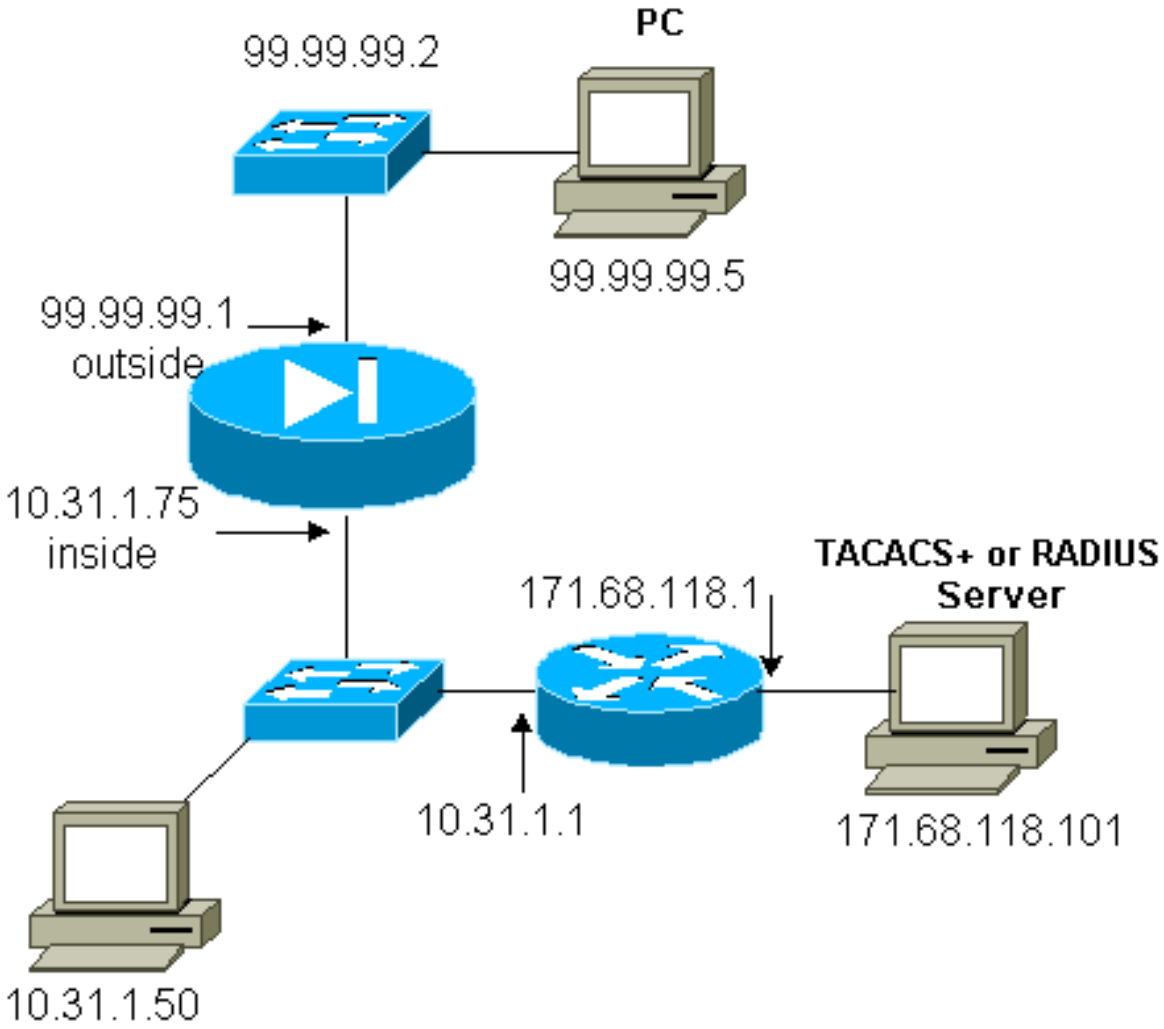
調試步驟

注意： Output Interpreter Tool(**僅供**註冊客戶使用)支援某些**show**命令，這允許您檢視**show**命令輸出的分析。

- 在新增AAA之前，確保PIX配置工作正常。如果您無法在建立驗證和授權之前傳遞流量，則以後將無法這樣做。

- 在PIX中啟用日誌記錄。日誌記錄控制檯調試不應在負載過重的系統上使用。可以使用logging buffered debugging，然後執行**show logging**命令。日誌記錄還可以傳送到系統日誌伺服器並在那裡檢視。
- 在TACACS+或RADIUS伺服器上啟用調試（所有伺服器均具有此選項）。

網路圖表



PIX配置

```
PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix3
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging timestamp
```

```
no logging standby
logging console debugging
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.7-99.99.99.10 netmask
255.255.255.0
nat (inside) 1 10.31.1.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp any any
conduit permit udp any any
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
route inside 171.68.118.0 255.255.255.0 10.31.1.1 1
route inside 171.68.120.0 255.255.255.0 10.31.1.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101
cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include telnet inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include http inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include ftp inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
```

```
terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca
: end
[OK]
```

來自PIX的身份驗證調試示例

本節顯示各種方案的身份驗證調試示例。

傳入

99.99.99.2的外部使用者起始流量到內部10.31.1.50(99.99.99)，並透過TACACS進行驗證（即傳入流量使用伺服器清單「AuthInbound」，其中包括TACACS伺服器171.68.118.101）。

PIX調試 — 良好身份驗證 — TACACS+

以下示例顯示了具有良好身份驗證的PIX調試：

```
109001: Auth start for user '???' from
    99.99.99.2/11008 to 10.31.1.50/23
109011: Authen Session Start: user 'cse', sid 4
109005: Authentication succeeded for user 'cse'
    from 10.31.1.50/23 to 99.99.99.e
302001: Built inbound TCP connection 10 for
    faddr 99.99.99.2/11008 gaddr 99.99.)
```

PIX調試 — 身份驗證錯誤（使用者名稱或密碼） — TACACS+

以下示例顯示帶有錯誤身份驗證（使用者名稱或密碼）的PIX調試。 使用者看到三個使用者名稱/密碼集，然後顯示以下訊息：。

```
109001: Auth start for user '???' from
     99.99.99.2/11010 to 10.31.1.50/23
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

PIX調試 — 可以Ping伺服器，無響應 — TACACS+

以下示例顯示了一個PIX調試，其中伺服器可以ping通，但不會與PIX通訊。使用者只看到一次使用者名稱，但PIX從不要求密碼（這是Telnet）。 使用者看到Error:。

```
109001: Auth start for user '???' from 99.99.99.2/11011
     to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
```

```
  109006: Authentication failed for user '' from 10.31.1.50/23
     to 99.99.99.2/11011 on interface outside
```

PIX調試 — 無法Ping伺服器 — TACACS+

以下示例顯示伺服器無法ping通的PIX調試。使用者只看到一次使用者名稱，但PIX從不要求密碼（這是Telnet）。 將顯示以下消息：TACACS+和數（配置中交換了偽伺服器）。

```
111005: console end configuration: OK
  109001: Auth start for user '???' from
     99.99.99.2/11012 to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11012 on interface
     outside
```

PIX調試 — 良好身份驗證 — RADIUS

以下示例顯示了具有良好身份驗證的PIX調試：

```
109001: Auth start for user '???' from
     10.31.1.50/11008 to 99.99.99.2/23
  109011: Authen Session Start: user 'pixuser', sid 8
  109005: Authentication succeeded for user
     'pixuser' from 10.31.1.50/11008 to
     99.99.99.2/23 on interface inside
  302001: Built outbound TCP connection 16 for faddr
     99.99.99.2/23 gaddr 99.99.99.99/11008
     laddr 10.31.1.50/11008 (pixuser)
```

PIX調試 — 身份驗證錯誤（使用者名稱或密碼） — RADIUS

以下示例顯示帶有錯誤身份驗證（使用者名稱或密碼）的PIX調試。 使用者看到使用者名稱和密碼的請求，並有三個輸入這些資訊的機會。當輸入不成功時，將顯示以下消息：。

```
109001: Auth start for user '???' from 10.31.1.50/11010
     to 99.99.99.2/23
  109006: Authentication failed for user ''
     from 10.31.1.50/11010 to 99.99.99.2/23
     on interface inside
```

PIX調試 — 可以Ping伺服器，守護程式關閉 — RADIUS

以下示例顯示了一個PIX調試，其中伺服器可以執行ping操作，但守護進程已關閉，不會與PIX通訊。使用者看到使用者名稱、密碼、RADIUS敗訊息和。錯誤消息。

```
109001: Auth start for user '???' from 10.31.1.50/11011
     to 99.99.99.2/23
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
```

```
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  09002: Auth from 10.31.1.50/11011 to 99.99.99.2/23
     failed (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11011
     to 99.99.99.2/23 on interface inside
```

PIX調試 — 無法Ping伺服器或金鑰/客戶端不匹配 — RADIUS

以下示例顯示一個PIX調試，其中伺服器不可以ping或存在客戶端/金鑰不匹配。使用者看到使用者名稱、密碼、RADIUS訊息和Error:務器時超出最大嘗試次數消息)。

```
109001: Auth start for user '???' from 10.31.1.50/11012
     to 99.99.99.2/23
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11012
     to 99.99.99.2/23 on interface inside
```

新增授權

如果您決定新增授權，由於授權在未經驗證的情況下無效，因此需要授權用於相同的源和目標範圍。

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

請注意，由於傳出流量已使用RADIUS進行身份驗證，且RADIUS授權無效，因此不為傳出新增授權。

來自PIX的身份驗證和授權調試示例

PIX調試 — 良好身份驗證和成功授權 — TACACS+

以下示例顯示了具有良好身份驗證和成功授權的PIX調試：

```
109001: Auth start for user '???' from 99.99.99.2/11016
   to 10.31.1.50/23
109011: Authen Session Start: user 'cse', Sid 11
109005: Authentication succeeded for user 'cse'
   from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
109011: Authen Session Start: user 'cse', Sid 11
109007: Authorization permitted for user 'cse' from
   99.99.99.2/11016 to 10.31.1.50/23 on interface outside
302001: Built inbound TCP connection 19 for faddr 99.99.99.2/11016
```

```
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

PIX調試 — 身份驗證良好，授權失敗 — TACACS+

以下示例顯示了具有良好身份驗證但授權失敗的PIX調試。使用者在此處還會看到消息Error:絕。

```
109001: Auth start for user '???' from
    99.99.99.2/11017 to 10.31.1.50/23
109011: Authen Session Start: user 'httponly',
   Sid 12
109005: Authentication succeeded for user 'httponly'
   from 10.31.1.50/23 to 99.99.99.2/11017 on
   interface outside
109008: Authorization denied for user 'httponly' from
   10.31.1.50/23 to 99.99.99.2/11017 on interface outside
```

新增記帳

TACACS+

```
aaa accounting include any inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

TACACS+免費軟體輸出：

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
   99.99.99.2 start task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
   99.99.99.2 stop task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet elapsed_time=5
   bytes_in=39 bytes_out=126
```

RADIUS

```
aaa accounting include any outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

Merit RADIUS輸出：

```
Tue Feb 22 08:56:17 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        User-Name = pixuser

        Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
```

```
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        Username = pixuser
        Acct-Session-Time = 6
        Acct-Input-Octets = 139
        Acct-Output-Octets = 36
```

使用排除命令

如果將另一台外部主機(99.99.99.100)新增到我們的網路，並且此主機受信任，則可以使用以下命令將其從身份驗證和授權中排除：

```
aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100
 255.255.255.255 AuthInbound

aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255
AuthInbound
```

最大會話數和檢視登入使用者

有些TACACS+和RADIUS伺服器具有「max-session」或「view logged-in users」功能。執行max-sessions或check logged-in使用者的功能取決於記帳記錄。當生成記帳「開始」記錄但沒有「停止」記錄時，TACACS+或RADIUS伺服器會假定該使用者仍然登入（即，使用者通過PIX具有會話）。

由於連線的性質，這非常適用於Telnet和FTP連線。由於連線的性質，HTTP無法順利運作。在以下示例中，使用了不同的網路配置，但概念是相同的。

使用者通過PIX進行遠端通訊，在途中進行身份驗證：

```
   171.68.118.100/1200 to 9.9.9.25 /23
  (pix) 109011: Authen Session Start: user
     'cse', Sid 3
  (pix) 109005: Authentication succeeded for user
     'cse' from 171.68.118.100/12 00 to 9.9.9.25/23
  (pix) 302001: Built TCP connection 5 for faddr
     9.9.9.25/23 gaddr 9.9.9.10/12 00
     laddr 171.68.118.100/1200 (cse)
  (server start account) Sun Nov 8 16:31:10 1998
     rtp-pinecone.rtp.cisco.com cse
  PIX 171.68.118.100 start task_id=0x3 foreign_ip=9.9.9.25
     local_ip=171.68.118.100 cmd=telnet
```

由於伺服器已看到一條開始記錄但沒有停止記錄，因此此時伺服器會顯示Telnet使用者已登入。如果使用者嘗試需要身份驗證的另一連線（可能從另一台PC進行），並且如果在該使用者的伺服器上將max-sessions設定為**1**（假定該伺服器支援max-sessions），伺服器將拒絕該連線。

使用者在目標主機上進行Telnet或FTP業務，然後退出（在那裡花費10分鐘）：

```
pix) 302002: Teardown TCP connection 5 faddr
     9.9.9.25/80 gaddr 9.9.9.10/128
  1 laddr 171.68.118.100/1281 duration 0:00:00
     bytes 1907 (cse)
```

```
  (server stop account) Sun Nov 8 16:41:17 1998
     rtp-pinecone.rtp.cisco.com cse
  PIX 171.68.118.100 stop task_id=0x3 foreign_ip=9.9.9.25
     local_ip=171.68.118.100
  cmd=telnet elapsed_time=5 bytes_in=98 bytes_out=36
```

無論uauth是0（即每次進行身份驗證）還是更多（在uauth期間進行一次身份驗證），都會為每個訪問的站點剪下記帳記錄。

由於通訊協定的性質，HTTP的運作方式不同。以下是HTTP的範例：

使用者通過PIX從171.68.118.100瀏覽到9.9.9.25:

```
(pix) 109001: Auth start for user '???' from
     171.68.118.100/1281 to 9.9.9.25 /80
  (pix) 109011: Authen Session Start: user 'cse', Sid 5
  (pix) 109005: Authentication succeeded for user
     'cse' from 171.68.118.100/12 81 to 9.9.9.25/80
  (pix) 302001: Built TCP connection 5 for faddr
     9.9.9.25/80 gaddr 9.9.9.10/12 81 laddr
     171.68.118.100/1281 (cse)
  (server start account) Sun Nov 8 16:35:34 1998
     rtp-pinecone.rtp.cisco.com cse
  PIX 171.68.118.100 start task_id=0x9 foreign_ip=9.9.9.25
     local_ip=171.68.118.100 cmd=http
  (pix) 302002: Teardown TCP connection 5 faddr
     9.9.9.25/80 gaddr 9.9.9.10/128
  1 laddr 171.68.118.100/1281 duration 0:00:00
     bytes 1907 (cse)
  (server stop account) Sun Nov 8 16:35.35 1998
     rtp-pinecone.rtp.cisco .com cse
  PIX 171.68.118.100 stop task_id=0x9 foreign_ip =9.9.9.25
  local_ip=171.68.118.100 cmd=http elapsed_time=0
     bytes_ in=1907 bytes_out=223
```

使用者讀取下載的網頁。

開始記錄發佈時間為16:35:34，停止記錄發佈時間為16:35:35。此下載僅需一秒（即，開始記錄與停止記錄之間的間隔不到一秒）。 使用者是否仍登入到該網站，並且當使用者正在讀取該網頁時連線仍然開啟？否。最大會話數或檢視登入的使用者是否在此處工作？否，因為HTTP中的連線時間（「已建立」和「拆除」之間的時間）太短。開始和停止記錄為亞秒。沒有停止記錄的開始記錄不存在，因為這些記錄實際上發生在同一時刻。無論uauth設定為0還是大於或等於0，仍會針對每個事務向伺服器傳送啟動和停止記錄。但是，由於HTTP連線的性質，最大會話數和檢視登入使用者數將無法工作。

在PIX本身進行身份驗證和啟用

前面的討論涉及通過PIX驗證Telnet（以及HTTP、FTP）流量。確保Telnet至PIX在未經身份驗證的情況下工作正常：

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

然後新增命令以驗證使用者Telnet到PIX:

```
aaa authentication telnet console AuthInbound
```

當使用者Telnet至PIX時，系統會提示他們輸入Telnet口令(**WW**)。 PIX還請求TACACS+或RADIUS使用者名稱和密碼。在這種情況下，由於使用了AuthInbound伺服器清單，PIX會請求TACACS+使用者名稱和密碼。

如果伺服器關閉，您可以通過輸入**pix**作為使用者名稱，然後輸入enable password(**enable password**隨意)來訪問PIX。 使用以下命令：

```
aaa authentication enable console AuthInbound
```

系統會提示使用者輸入傳送到TACACS或RADIUS伺服器的使用者名稱和密碼。在這種情況下，由於使用了AuthInbound伺服器清單，PIX會請求TACACS+使用者名稱和密碼。

由於用於啟用的身份驗證資料包與用於登入的身份驗證資料包相同，因此，如果使用者可以使用TACACS或RADIUS登入到PIX，則可以使用相同的使用者名稱/密碼通過TACACS或RADIUS啟用。此問題已分配給Cisco錯誤ID CSCdm47044(僅限註冊客戶)。

如果伺服器關閉，您可以通過從PIX輸入**pix**作為使用者名稱和普通啟用密碼(**enable password**隨意)來訪問PIX啟用模式。 如果**enable password** 不包含PIX配置中的任何值，請輸入**pix**作為使用者名稱，然後按**Enter**。如果已設定啟用密碼但不知道該密碼，則需要構建密碼恢復磁碟以重置密碼。

更改提示使用者檢視

如果您有以下命令：

```
auth-prompt PIX_PIX_PIX
```

使用者通過PIX可以看到以下順序：

```
PIX_PIX_PIX [at which point one would enter the username]
   Password:[at which point one would enter the password]
```

到達最終目的地後，使用者會看到使用者名稱：和密碼：目標框顯示的提示。此提示僅影響使用者通*過*PIX，而不影響到PIX。

注意：沒有針對訪問PIX而削減的記帳記錄。

自定義使用者在成功/失敗時看到的消息

如果您有以下命令：

```
auth-prompt accept "GOOD_AUTH"
auth-prompt reject "BAD_AUTH"
```

然後使用者通過PIX登入失敗/成功時看到以下序列：

```
PIX_PIX_PIX
   Username: asjdkl
   Password: "BAD_AUTH"
   "PIX_PIX_PIX"
   Username: cse
   Password: "GOOD_AUTH"
```

每使用者空閒和絕對超時

此功能目前無法運作，且問題已指派為Cisco錯誤ID CSCdp93492(僅限註冊客戶)。

虛擬HTTP

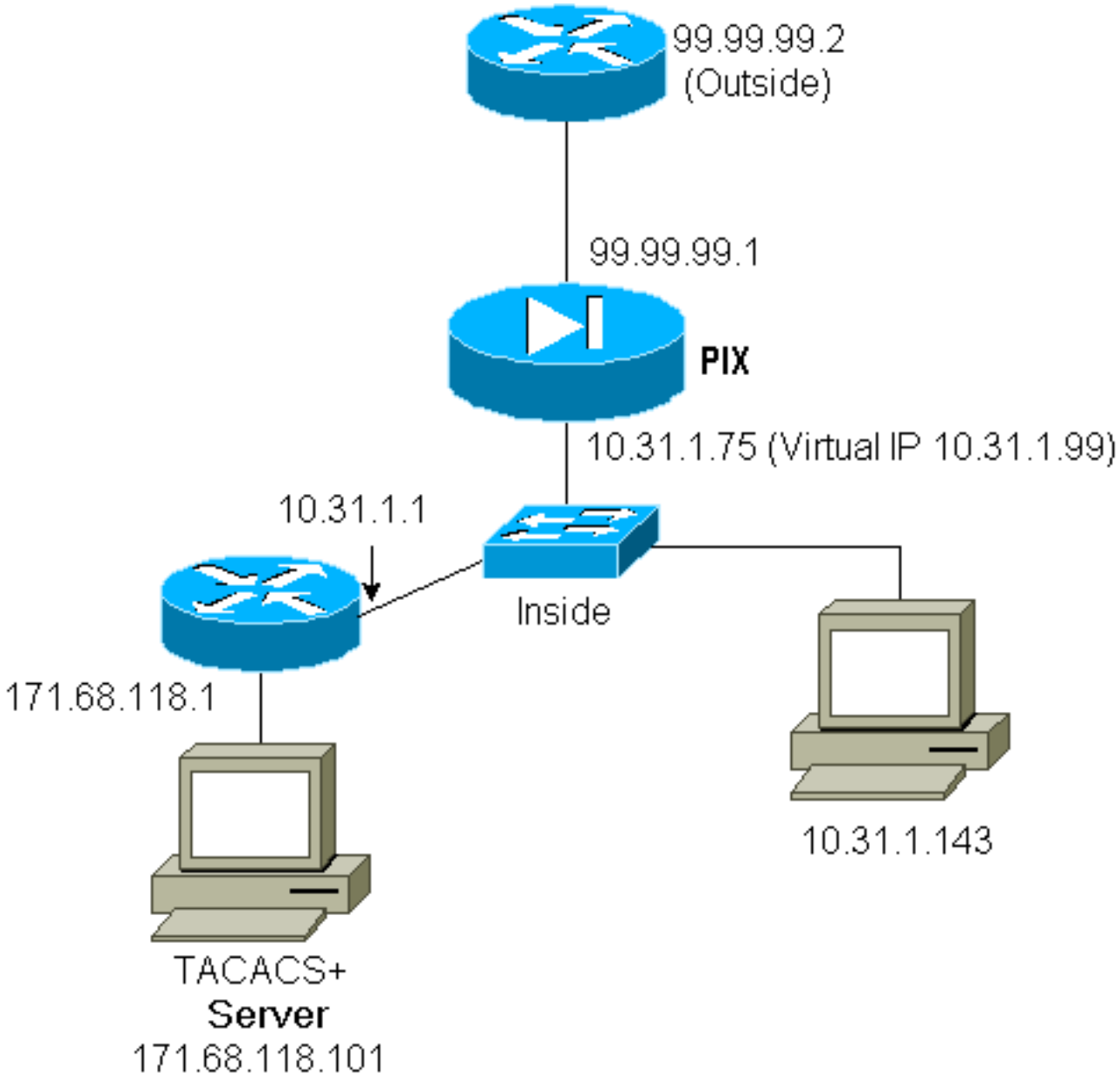
如果在PIX外部的站點以及PIX本身需要身份驗證，有時可能會觀察到異常的瀏覽器行為，因為瀏覽器會快取使用者名稱和密碼。

要避免這種情況，可以使用以下命令向PIX配置中新增一個RFC 1918 地址（即，在Internet上不可路由，但對PIX內部網路有效且唯一的地址）來實施虛擬HTTP:

```
virtual http #.#.#.# [warn]
```

當使用者嘗試離開PIX時，需要進行身份驗證。如果存在warn引數，則使用者會收到重新導向訊息。驗證對uauth中的時間長度沒有影響。如文檔所示，請勿使用虛擬HTTP將**timeout uauth**命令持續時間設定為0秒；這可以防止與實際Web伺服器的HTTP連線。

虛擬HTTP出站示例



PIX配置虛擬HTTP出站：

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 01:00:00
aaa authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
virtual http 10.31.1.99
```

虛擬Telnet

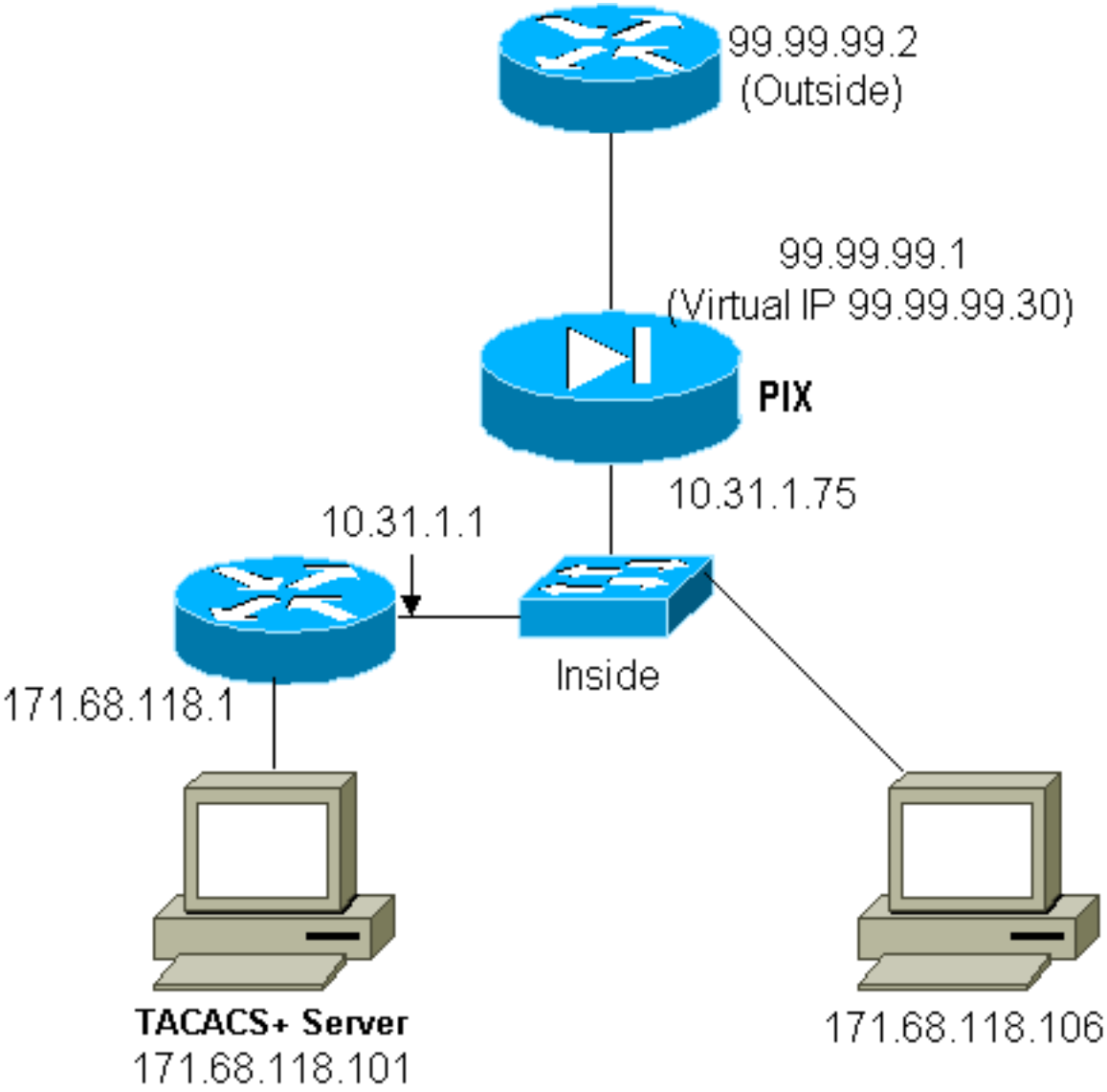
可以將PIX配置為對所有入站和出站進行身份驗證，但是這不是一個好主意，因為有些協定（如郵件）不容易進行身份驗證。當所有通過PIX的流量都經過身份驗證時，郵件伺服器和客戶端嘗試通過PIX通訊時，用於不可驗證協定的PIX系統日誌顯示如下消息：

```
109013: User must authenticate before using
    this service
109009: Authorization denied from 171.68.118.106/49
    to 9.9.9.10/11094    (not authenticated)
```

但是，如果確實需要對某種異常服務進行身份驗證，可以使用**virtual telnet**命令完成此操作。此命令允許對虛擬Telnet IP地址進行身份驗證。進行此驗證後，異常服務的流量可以進入實際伺服器。

在本例中，您希望TCP埠49流量從外部主機99.99.99.2流向內部主機171.68.118.106。由於此流量並非真正可身份驗證，因此請設定虛擬Telnet。對於虛擬Telnet，必須存在關聯的靜態。這裡，99.99.99.20和171.68.118.20都是虛擬地址。

虛擬Telnet傳入



PIX配置虛擬Telnet入站

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
static (inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0
```

```
conduit permit tcp host 99.99.99.20 eq telnet any
conduit permit tcp host 99.99.99.30 eq tacacs any
aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+
aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
aaa authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
virtual telnet 99.99.99.20
```

PIX調試虛擬Telnet入站

位於99.99.99.2的使用者必須首先通過Telnet對PIX上的99.99.99.20地址進行身份驗證：

```
109001: Auth start for user '???' from
    99.99.99.2/22530 to 171.68.118.20/23
 109011: Authen Session Start: user 'cse', Sid 13
 109005: Authentication succeeded for user
    'cse' from 171.68.118.20/23 to
    99.99.99.2/22530 on interface outside
```

成功驗證後，**show uauth**命令會顯示使用者有「計量器上的時間」：

```
pixfirewall# show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.2, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

當位於99.99.99.2的裝置要將TCP/49流量傳送到位於171.68.118.106的裝置時：

```
302001: Built inbound TCP connection 16
    for faddr 99.99.99.2/11054 gaddr
    99.99.99.30/49 laddr 171.68.118.106/49 (cse)
```

可以新增授權：

```
aaa authorization include tcp/49 inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

因此，當嘗試通過PIX進行TCP/49流量時，PIX還會向伺服器傳送授權查詢：

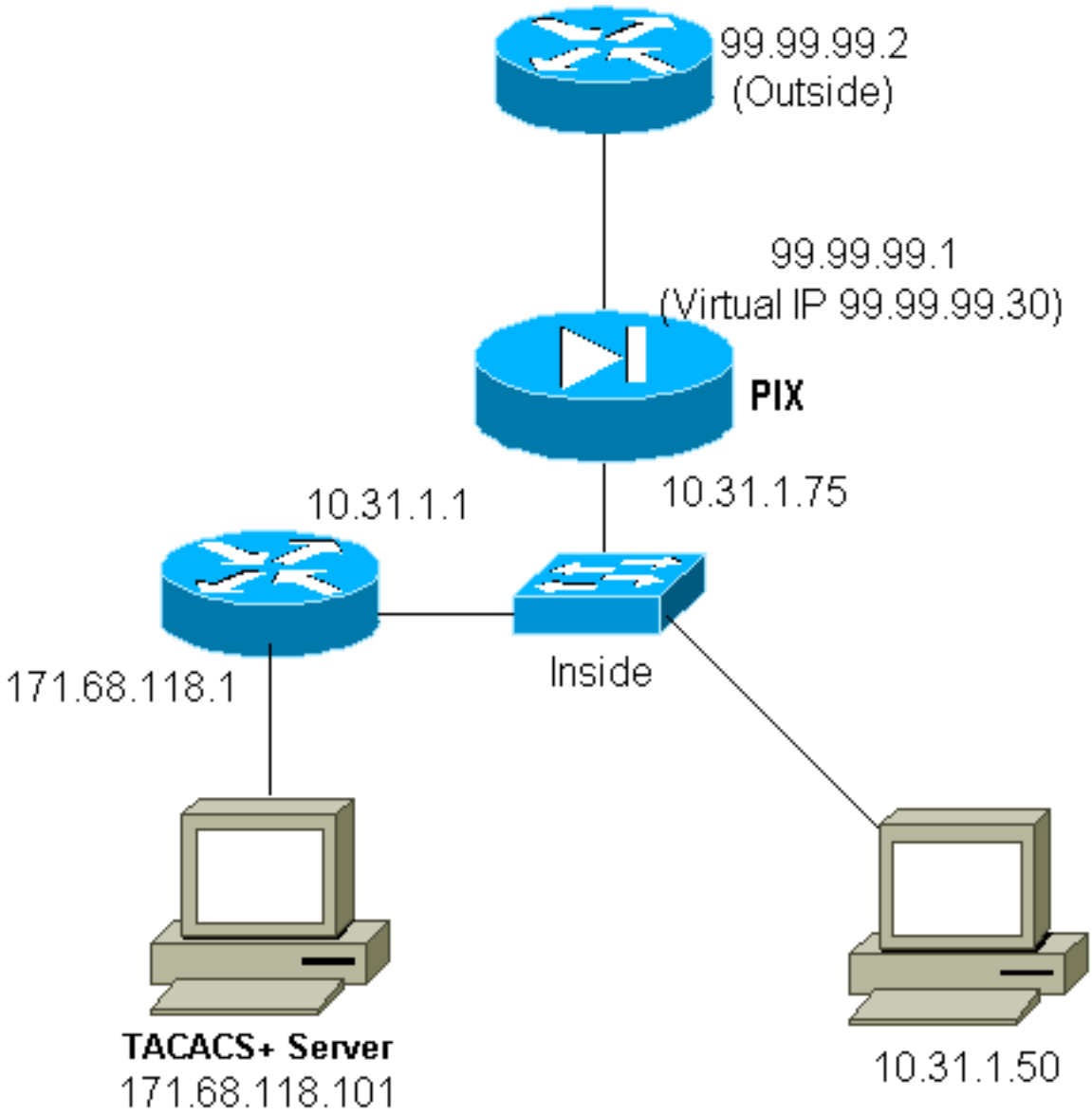
```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

在TACACS+伺服器上，這顯示為：

```
service=shell,
  cmd=tcp/49,
  cmd-arg=171.68.118.106
```

虛擬Telnet出站

由於預設情況下允許出站流量，因此使用虛擬Telnet出站不需要靜態。在以下示例中，位於10.31.1.50 Telnet的內部使用者連線到虛擬99.99.99.30並進行身份驗證；telnet連線會立即捨棄。通過驗證後，允許從10.31.1.50到地址為99.99.99.2的伺服器的TCP流量：



PIX配置虛擬Telnet出站：

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 0:05:00 absolute
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
virtual telnet 99.99.99.30
```

注意：沒有授權，因為這是RADIUS。

PIX調試虛擬Telnet出站：

```
109001: Auth start for user '???' from 10.31.1.50/11034
   to 99.99.99.30/23
 109011: Authen Session Start: user 'pixuser', Sid 16
 109005: Authentication succeeded for user 'pixuser'
   from 10.31.1.50/11034 to 99.99.99.30/23 on interface
   inside
 302001: Built outbound TCP connection 18 for faddr
   99.99.99.2/49 gaddr 99.99.99.8/11036 laddr
   10.31.1.50/11036 (pixuser)
 302002: Teardown TCP connection 18 faddr 99.99.99.2/49
   gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
   duration 0:00:02 bytes 0 (pixuser)
```

虛擬Telnet註銷

使用者通過Telnet連線至虛擬Telnet IP位址時，**show uauth**指令會顯示其uauth。如果使用者希望在其會話完成之後在uauth中還有時間時阻止流量通過，則需要再次通過Telnet連線到虛擬Telnet IP地址。這會關閉作業階段。

首次驗證後：

```
 pix3# show uauth
                        Current    Most Seen
 Authenticated Users       1          2
 Authen In Progress        0          1
 user 'pixuser' at 10.31.1.50, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
 pix3# 109001: Auth start for user 'pixuser' from
   10.31.1.50/11038 to 99.99.99.30/23
 109005: Authentication succeeded for user 'pixuser'
   from 10.31.1.50/11038 to 99.99.99.30/23 on
   interface inside
```

第二次驗證後（即，將孔切換為關閉狀態）：

```
 pix3# show uauth
                        Current    Most Seen
 Authenticated Users       0          2
 Authen In Progress        0          1
```

連線埠授權

允許對連線埠範圍（例如TCP/30-100）進行授權。 如果在PIX上配置了虛擬Telnet並對一系列埠進行了授權，一旦使用虛擬Telnet開啟了孔，PIX就會向TACACS+伺服器發出**tcp/30-100**命令進行授權：

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.75 host 99.99.99.2
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
virtual telnet 99.99.99.75
aaa authentication include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

```
aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
virtual telnet 99.99.99.30
```

TACACS+免費軟體伺服器配置：

```
user = anyone {
         login = cleartext "anyone"
         cmd = tcp/30-100 {
         permit 10.31.1.50
         }
         }
```

除HTTP、FTP和Telnet以外的流量的AAA記帳

在確保虛擬Telnet工作以允許到網路內部主機的TCP/49流量之後，我們決定對此進行記帳，因此我們補充說：

```
aaa accounting include any inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

這會導致在tcp/49流量通過（此範例來自TACACS+免費軟體）時剪下記帳記錄：

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
    99.99.99.2 start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106
    cmd=tcp/49
```

延伸驗證(Xauth)

配置示例

- 使用Xauth終止多個Cisco安全PIX防火牆介面上的IPSec隧道
- Cisco Secure PIX防火牆與具有擴展身份驗證的VPN客戶端之間的IPSec

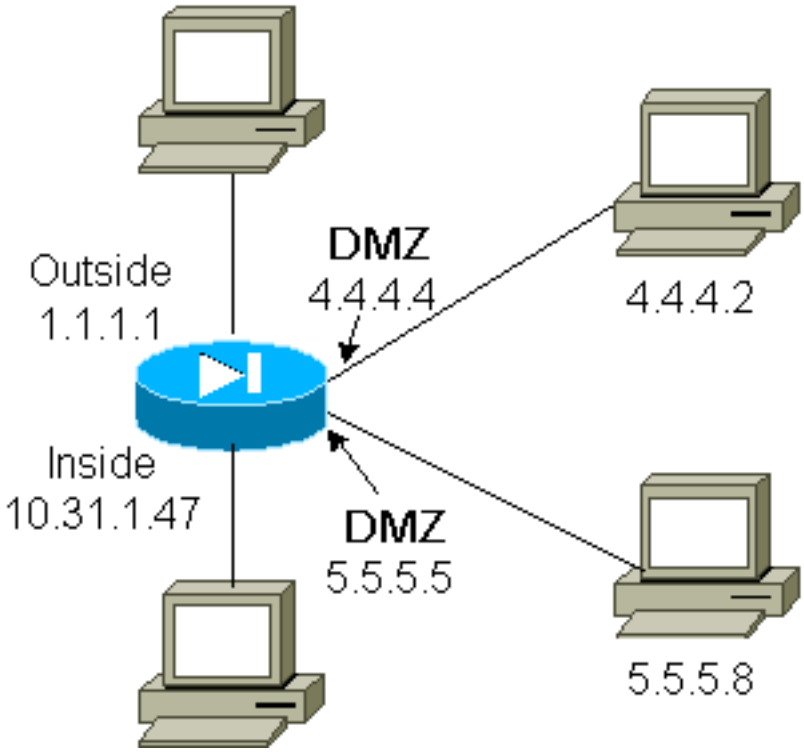
DMZ上的身份驗證

要驗證從一個DMZ介面到另一個介面的使用者，請通知PIX驗證指定介面的流量。我們的PIX安排如下：

```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2

pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47
```

most secure

網路圖表



PIX配置

我們希望對pix/intf4和pix/intf5之間的Telnet流量進行身份驗證：

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
(nameif ethernet2 pix/intf2 security10
nameif ethernet3 pix/intf3 security15)
nameif ethernet4 pix/intf4 security20
nameif ethernet5 pix/intf5 security25
ip address outside 1.1.1.1 255.255.255.0
ip address inside 10.31.1.47 255.255.255.0
(ip address pix/intf2 127.0.0.1 255.255.255.255
ip address pix/intf3 127.0.0.1 255.255.255.255)
ip address pix/intf4 4.4.4.4 255.255.255.0
ip address pix/intf5 5.5.5.5 255.255.255.0
static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask 255.255.255.255 0 0
aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa-server TACACS+ protocol tacacs+
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

Xauth記帳

如果在PIX中使用xauth配置了**sysopt connection permit-ipsec**命令(而不是**sysopt ipsec pl-compatible**命令)，則記帳對於TCP連線有效，但對於ICMP或UDP無效。

相關資訊

- PIX產品支援頁
- PIX命令參考
- RADIUS 支援頁面
- 要求建議 (RFC)
- Cisco Secure UNIX支援頁
- Cisco Secure ACS for Windows支援頁
- 技術支援 - Cisco Systems